AMENDMENTS TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of the claims.

Listing of Claims:

Claims 1-222 (Canceled).

Claim 223. (Currently Amended) A method for enabling access to one or more resources within a computer network, comprising the steps of:

assigning a unique user identifier to each authorized human user of the computer network;

upon initiation of a TCP/IP communication attempt at a source node initiated by a specific authorized human user for access to a specific resource within the computer network, wherein the TCP/IP communication attempt includes a synchronization packet having a header, inserting the unique user identifier of the specific authorized human user into the header of the synchronization packet at the source node;

intercepting the synchronization packet within the computer network;

extracting the unique user identifier from the header of the synchronization packet to identify the specific authorized human user initiating the TCP/IP communication attempt; and

granting the specific authorized human user access to the specific resource at a destination node within the computer network as a function of the unique user identifier extracted from the header.

Claim 224. (Previously Presented) The method of claim 223 wherein data identifying the unique user identifier is included in a sequence number field of the header of the synchronization packet.

Claim 225. (Previously Presented) The method of claim 223 wherein the unique user identifier is included in an acknowledgement field of the header of the synchronization packet.

Claim 226. (Previously Presented) The method of claim 225 wherein data in the acknowledgement field has a non-zero value.

Claim 227. (Currently Amended) The method of claim 223 wherein the unique user identifier comprises a user name of the specific authorized human user.

Claim 228. (Previously Presented) The method of claim 223 further comprising the step of encrypting the unique user identifier prior to inserting the unique user identifier into the header of the synchronization packet.

Claim 229. (Previously Presented) The method of claim 228 further comprising the step of decrypting the unique user identifier after intercepting the synchronization packet.

Claim 230. (Previously Presented) The method of claim 223 further comprising the step of recording the TCP/IP communication attempt in a database.

Claim 231. (Previously Presented) The method of claim 223 further comprising the step of notifying a network administrator if the TCP/IP communication attempt is not granted.

Claim 232. (Previously Presented) The method of claim 223 further comprising the step of logging the TCP/IP communication attempt.

Claim 233. (Previously Presented) The method of claim 223 wherein the specific resource is a database.

Claim 234. (Previously Presented) The method of claim 223 wherein the specific resource is an application.

Claim 235. (Previously Presented) The method of claim 223 wherein the specific resource is an authorized computer within the computer network.

Claim 236. (Currently Amended) The method of claim 223 wherein the unique user identifier indicates an authorized human user associated with [[a]] the source node.

Claim 237. (Currently Amended) The method of claim 236 wherein the specific resource is [[a]] the destination node.

Claim 238. (Currently Amended) A method for preventing unauthorized access to one or more resources within a computer network, wherein the computer network includes a plurality of authorized human users and wherein a unique user identifier is assigned to each of the plurality of authorized human users, comprising the steps of:

maintaining the plurality of unique user identifiers in a database;

intercepting a TCP/IP communication attempt from an undetermined user, wherein the TCP/IP communication attempt includes a synchronization packet having a header and wherein the TCP/IP communication represents a request for access to a specific resource within the computer network;

obtaining data from the header of the synchronization packet;

comparing the data obtained from the header with the plurality of unique user identifiers maintained in the database to determine if the undetermined user is one of the plurality of authorized human users logged into an authorized computer of the computer network; and

denying the request for access to the specific resource if the data obtained from the header does not match one of the plurality of unique user identifiers in the database.

Claim 239. (Previously Presented) The method of claim 238 wherein data identifying the unique user identifier is included in a sequence number field of the header of the synchronization packet.

Claim 240. (Previously Presented) The method of claim 238 wherein the unique user identifier is included in an acknowledgement field of the header of the synchronization packet.

Claim 241. (Previously Presented) The method of claim 240 wherein data in the acknowledgement field has a non-zero value.

Claim 242. (Currently Amended) The method of claim 238 wherein the unique user identifier comprises a user name of [[the]] a specific authorized human user.

Claim 243. (Previously Presented) The method of claim 238 further comprising the step of recording the TCP/IP communication attempt in a database.

Claim 244. (Previously Presented) The method of claim 238 further comprising the step of notifying a network administrator if the TCP/IP communication attempt is denied.

Claim 245. (Previously Presented) The method of claim 238 further comprising the step of logging the TCP/IP communication attempt if the TCP/IP communication attempt is denied.

Claim 246. (Previously Presented) The method of claim 238 wherein the specific resource is a database.

Claim 247. (Previously Presented) The method of claim 238 wherein the specific resource is an application.

Claim 248. (Previously Presented) The method of claim 238 wherein the specific resource is an authorized computer within the computer network.

Claim 249. (Currently Amended) The method of claim 238 wherein the unique user identifier indicates an authorized human user associated with a source node.

Claim 250. (Previously Presented) The method of claim 249 wherein the specific resource is a destination node.

Claim 251. (Currently Amended) A method for managing communications within a computer network, comprising the steps of:

assigning a unique user identifier to each authorized human user of the computer network;

upon initiation of a TCP/IP communication attempt by a specific authorized human user accessing a specific source node of the computer network, wherein the TCP/IP communication attempt is targeted to a destination node of the computer network and wherein the TCP/IP communication attempt includes a synchronization packet having a header, inserting the unique user identifier of the specific authorized human user into the header of the synchronization packet;

intercepting the synchronization packet within the computer network prior to receipt by the destination node;

extracting the unique user identifier from the header of the synchronization packet to identify the specific authorized human user initiating the TCP/IP communication attempt; and

enabling the TCP/IP communication between the specific source node and the destination node as a function of the unique user identifier extracted from the header.

Claim 252. (Previously Presented) The method of claim 251 wherein data identifying the unique user identifier is included in a sequence number field of the header of the synchronization packet.

Claim 253. (Previously Presented) The method of claim 251 wherein the unique user identifier is included in an acknowledgement field of the header of the synchronization packet.

Claim 254. (Previously Presented) The method of claim 253 wherein data in the acknowledgement field has a non-zero value.

Claim 255. (Previously Presented) The method of claim 251 further comprising the step of encrypting the unique user identifier prior to inserting the unique user identifier into the header of the synchronization packet.

Claim 256. (Previously Presented) The method of claim 255 further comprising the step of decrypting the unique user identifier after intercepting the synchronization packet.

Claim 257. (Previously Presented) The method of claim 251 further comprising the step of recording the TCP/IP communication attempt in a database.

Claim 258. (Previously Presented) The method of claim 251 further comprising the step of notifying a network administrator if the TCP/IP communication attempt is not enabled.

Claim 259. (Previously Presented) The method of claim 251 further comprising the step of logging the TCP/IP communication attempt.

Claim 260. (Currently Amended) The method of claim 251 wherein the specific source node is associated with [[a]] the specific authorized human user of the computer network.

Claim 261. (Currently Amended) The method of claim 251 wherein the receiving node is associated with another specific authorized human user of the network.

Claim 262. (Currently Amended) A method for managing communications within a computer network, comprising the steps of:

assigning a unique user identifier to each authorized human user of the computer network;

assigning a unique source identifier to each authorized computer within the computer network;

upon initiation of a TCP/IP communication attempt initiated by a specific authorized human user logged in to a specific authorized computer, wherein the TCP/IP communication attempt is targeted to a destination node in the computer network and wherein the TCP/IP communication attempt includes a synchronization packet having a header, inserting the unique user identifier of the specific authorized human user and the unique source identifier of the specific authorized computer into the header of the synchronization packet;

intercepting the synchronization packet within the computer network prior to receipt by the destination node;

extracting the unique user identifier and unique source identifier from the header of the synchronization packet to identify the specific authorized human user and the specific authorized computer initiating the TCP/IP communication attempt; and

allowing the TCP/IP communication attempt with the destination node if the specific authorized human user and specific authorized computer are each authorized to communicate with the destination node

based on the unique user identifier and unique source identifier extracted from the header.

Claim 263. (Previously Presented) The method of claim 262 wherein data identifying the unique user identifier is included in a sequence number field of the header of the synchronization packet.

Claim 264. (Previously Presented) The method of claim 262 wherein the unique user identifier is included in an acknowledgement field of the header of the synchronization packet.

Claim 265. (Previously Presented) The method of claim 264 wherein data in the acknowledgement field has a non-zero value.

Claim 266. (Previously Presented) The method of claim 262 wherein data identifying the unique source identifier is included in an acknowledgement field of the synchronization packet.

Claim 267. (Previously Presented) The method of claim 266 wherein data in the acknowledgement field has a non-zero value.

Claim 268. (Currently Amended) The method of claim 262 wherein the unique user identifier comprises a user name of the specific authorized human user.

Claim 269. (Previously Presented) The method of claim 262 further comprising the step of encrypting the unique user identifier prior to inserting the unique user identifier into the header of the synchronization packet.

Claim 270. (Previously Presented) The method of claim 269 further comprising the step of decrypting the unique user identifier after intercepting the synchronization packet.

Claim 271. (Currently Amended) The method of claim 262 wherein the unique source identifier is assigned based on one or more constant identifiers obtained from hardware associated with a respective authorized computer.

Claim 272. (Previously Presented) The method of claim 262 further comprising the step of encrypting the unique source identifier prior to inserting the unique source identifier into the header of the synchronization packet.

Claim 273. (Previously Presented) The method of claim 272 further comprising the step of decrypting the unique source identifier after intercepting the synchronization packet.

Claim 274. (Previously Presented) The method of claim 262 further comprising the step of recording the TCP/IP communication attempt in a database.

Claim 275. (Previously Presented) The method of claim 262 further comprising the step of notifying a network administrator if the TCP/IP communication attempt is not allowed.

Claim 276. (Previously Presented) The method of claim 262 further comprising the step of logging the TCP/IP communication attempt if the TCP/IP communication attempt is not allowed.

Claim 277. (Previously Presented) The method of claim 262 wherein the destination node is an authorized computer within the computer network.

Claim 278. (Currently Amended) A method for managing communications within a computer network, comprising the steps of:

assigning a unique user identifier to each authorized human user of the computer network;

upon initiation of a TCP/IP communication attempt initiated by a specific authorized human user at a source node for access to a specific resource at a destination node within the computer network, wherein the TCP/IP communication attempt includes a synchronization packet having a header, inserting the unique user identifier of the specific authorized human user into the header of the synchronization packet;

intercepting the synchronization packet within the computer network;

extracting the unique user identifier from the header of the synchronization packet to identify the specific authorized human user initiating the TCP/IP communication attempt; and

logging the TCP/IP communication attempt and the unique user identifier in a database.

Claim 279. (Currently Amended) The method of claim 278 further comprising the step of granting the specific authorized human user access to the specific resource within the computer network as a function of the unique user identifier extracted from the header.

Claim 280. (Previously Presented) The method of claim 278 wherein data identifying the unique user identifier is included in a sequence number field of the header of the synchronization packet.

Claim 281. (Previously Presented) The method of claim 278 wherein the unique user identifier is included in an acknowledgement field of the header of the synchronization packet.

Claim 282. (Previously Presented) The method of claim 281 wherein data in the acknowledgement field has a non-zero value.

Claim 283. (Currently Amended) The method of claim 278 wherein the unique user identifier comprises a user name of the specific authorized human user.

Claim 284. (Previously Presented) The method of claim 278 further comprising the step of encrypting the unique user identifier prior to inserting the unique user identifier into the header of the synchronization packet.

Claim 285. (Previously Presented) The method of claim 284 further comprising the step of decrypting the unique user identifier after intercepting the synchronization packet.

Claim 286. (Previously Presented) The method of claim 279 further comprising the step of notifying a network administrator if the TCP/IP communication attempt is not granted.

Claim 287. (Previously Presented) The method of claim 278 wherein the specific resource is a database.

Claim 288. (Previously Presented) The method of claim 278 wherein the specific resource is an application.

Claim 289. (Previously Presented) The method of claim 278 wherein the specific resource is an authorized computer within the computer network.

Claim 290. (Currently Amended) The method of claim 278 wherein the unique user identifier indicates an authorized human user associated with [[a]] the source node.

Claim 291. (Currently Amended) The method of claim 290 wherein the specific resource is [[a]] the destination node.